Saving Space by Algebraization

Daniel Lokshtanov, Jesper Nederlof

Definitions: For an integer i let us $\mathbb{N}_i$ denote the set of integers $\{0,\dots,i-1\}$ and $\mathbb{Z}_i$ ring of integers modulo i. For sets A and B, the set $A[B]$ is the set of all functions $f: B \to A$. For a vector $v \in \mathbb{N}^d$ the set $\mathbb{N}_v$ is $\mathbb{N}_{v[0]} \times \mathbb{N}_{v[1]} \times \dots \times \mathbb{N}_{v[d-1]}$.

The vectors are instantiated using $\langle$ and $\rangle$. The $=$, $\leq$ and $<$ relations for vectors are pointwise. The *absolute value* of a complex number u and the length of a vector v is denoted by $||u||$ and $||v||$. When working with rings and semi-rings, $+$ denotes addition and $\cdot$ multiplication. For vectors, $\cdot$ means the *dot product*. When working with elements of $A[B]$ where A comes with addition and multiplication, we define *pointwise addition* operator $\oplus$ and *pointwise multiplication* operator $\odot$ as follows: $\forall x,y \in A[B], b \in B : (x \oplus y)[b] = x[b] + y[b]$ and $(x \odot y)[b] = x[b] \cdot y[b]$.

We use *Iverson's bracket notation*, so for a predicate b, $[b]$ is 1 if b is true and 0 otherwise. We will use this notation for singleton constants, in a form of $[X = y]v$, which is v if $X = y$ and 0 otherwise.

For a set S and binary operators O_1, O_2 on S, a *circuit* C over $(S; O_1, O_2)$ is a directed acyclic graph with parallel arcs, such that every node is either a *constant* gate, O_1 gate or O_2 gate. The constant gates have indegree 0 and are labelled with elements of S. The O_i gates have indegree 2 and its two in-neighbours are its *children*. The *output* of a constant gate is the element it is labelled with, the output of an O_i gate is the result of performing O_i on its two children. One gate c of C is marked as *output gate* and the output of C is the output of c. The *depth* $\Delta(C)$ is the size of the longest path, and the *size* of C is the size of the underlying graph.

Definition: For every $n \in \mathbb{N}^d$, the Discrete Fourier Transform is a linear transform $\mathcal{F}: \mathbb{C}[\mathbb{N}_n] \to \mathbb{C}[\mathbb{N}_n]$. Let $t \in \mathbb{C}^d$ so that $t[j] = 2\pi i/n[j]$ and let $N = \prod_{i=0}^{d-1} n[i]$. Then for $a \in \mathbb{C}[\mathbb{N}_n]$ we define $\mathcal{F}(a)$ and $\mathcal{F}^{-1}(a)$ as

$$\mathcal{F}(a)[x] = \sum_{j \in \mathbb{N}_n} e^{(x \odot t)\cdot j} a[j], \qquad \mathcal{F}^{-1}(a)[x] = \frac{1}{N} \sum_{j \in \mathbb{N}_n} e^{-(x \odot t)\cdot j} a[j].$$

Definition: For $a, b \in \mathbb{Z}[\mathbb{N}_n]$ we define *convolution of a, b*, $a \otimes b$, as

$$(a \otimes b)[x] = \sum_{0 \leq j \leq x} a[j] b[x-j].$$

The convolution *overflows* if there are vectors $x, y \in \mathbb{N}_n$, such that $a[x] \neq 0$, $b[y] \neq 0$ and $x + y \not< n$.

Theorem 4.2: For $a, b \in \mathbb{C}[\mathbb{N}_n]$ such that $a \otimes b$ does not overflow, $\mathcal{F}(a \otimes b) = \mathcal{F}(a) \odot F(b)$.

Theorem 4.3: Let $n \in \mathbb{N}^d$, $N = |\mathbb{N}_n|$, and C be a circuit over $(\mathbb{Z}[\mathbb{N}_n]; \oplus, \otimes)$ with only singleton constants. Suppose that for any gate $c \in C : \forall x \in \mathbb{N}_n, |c[x]| \leq m$ and that no convolution gate overflows. Let f be the output of C. Then, given n, m and $g \in \mathbb{N}_n$ we can compute $f[g]$ in time $\tilde{\mathcal{O}}((|C| N \log N) \log(Nm) \Delta(C))$ and space $\mathcal{O}((|C| + \log N) \log(Nm) \Delta(C))$.

Claim: Let C be a circuit over $(\mathbb{C}; +, \cdot)$ and $m, \ell \in \mathbb{N}$, such that for any gate $v \in C : ||v|| \leq m$. Suppose that $2^\ell \cdot (4m)^{\Delta(C)} \leq 1$. Then if we are given estimations of constants with ℓ-bit precision, we can compute the estimation of result with error at most $2^\ell \cdot (4m)^{\Delta(C)}$.

Problem Subset Sum
Instance: Set S of positive integers $w_1, \dots, w_n$, an integer w.
Question: Does there exist a subset $S' \subseteq S$ such that $\sum_{w_i \in S'} w_i = w$?

$$s_1 = [x = 0] \oplus [x = w_1]$$
$$s_i = s_{i-1} \oplus (s_{i-1} \otimes [x = w_i]) = s_{i-1} \otimes ([x = 0] \oplus [x = w_i])$$
$$s_n = ([x = 0] \oplus [x = w_1]) \otimes ([x = 0] \oplus [x = w_2]) \otimes \dots \otimes ([x = 0] \oplus [x = w_n])$$

Problem Knapsack
Instance: Set S of n pairs of positive integers $(v_1, w_1), \dots, (v_n, w_n)$, two positive integers v, w.
Question: Does there exist a subset $S' \subseteq \mathbb{N}_n$ such that $\sum_{i \in S'} v_i \geq v$ and $\sum_{i \in S'} w_i \leq w$?

$$s_1 = [x = \langle v, 0 \rangle] \oplus [x = \langle v - v_1, w_1 \rangle]$$
$$s_i = s_{i-1} \otimes ([x = \langle v, 0 \rangle] \oplus [x = \langle v - v_i, w_i \rangle])$$
$$(s_n \otimes [x \leq \langle nv - v, w \rangle])[\langle nv - v, w \rangle]$$

where $[x \leq p] = [x \leq \lfloor p/2 \rfloor] \otimes [x \leq \lfloor p/2 \rfloor] \oplus [x = p]$ and $[x \leq \langle a, b \rangle] = [x \leq \langle a, 0 \rangle] \otimes [x \leq \langle 0, b \rangle]$.

Definitions: Let V be a set and $\mathcal{R}$ be a ring. We will consider circuits over $(\mathcal{R}[2^V]; \oplus, \diamond)$, where $\diamond$ is the *union product* defined as

$$(a \diamond b)[Y] = \sum_{A \cup B = Y} a[A]b[B].$$

For $f \in \mathcal{R}[2^V]$, the *zeta-transform* ζf and the *Möbius-transform* μf are defined as follows:

$$\zeta f[Y] = \sum_{X \subseteq Y} f[Y], \qquad \mu f[Y] = \sum_{x \subseteq Y} (-1)^{|Y \setminus X|} f[X]$$

Lemma 5.1: For any function $f \in \mathcal{R}[2^V]$ holds that $\mu(\zeta f) = f$.

Lemma 5.2: For any functions $f, g \in \mathcal{R}[2^V]$ holds that $\zeta(f \diamond g) = (\zeta f) \odot (\zeta g)$.

Lemma 5.3: Let C be a circuit over $(\mathcal{R}[2^V]; \oplus, \diamond)$ and outputs s. Then there is a polynomial time algorithm that, given $Y \subseteq V$, creates circuit C' over $(\mathbb{R}; +, \cdot)$ with the same underlying graph, such that the output of C' is $(\zeta s)[Y]$.

Definition: Let V be a set, $\mathcal{R}$ a ring and $f, g \in \mathcal{R}[2^V]$. The operator *subset convolution* $*$ is defined as

$$(f * g)[Y] = \sum_{X \subseteq Y} f[X]g[Y \setminus X].$$

Theorem 5.1: Let v be a set and let C be a circuit over $(\mathbb{Z}[2^V]; \oplus, *)$. Suppose C outputs s, all its constants are singletons and m is an integer such that $s[V] \le m$. Then, given C and m, $s[V]$ can be computed using $\mathcal{O}^*(2^{|V|})$ and $\mathcal{O}(|V||C| \log m)$ space.

Problem UNWEIGHTED STEINER TREE
Instance: A graph $G = (V, E)$, $T \subseteq V$, an integer $t \le |V|$.
Question: Does there exist a subtree (V', E') of G such that $|V'| \le t$ and $T \subseteq V'$?

$$f_1^v = [X = \emptyset] \text{ for } v \notin T \qquad f_1^v = [X = \{v\}] \oplus [X = \emptyset] \text{ for } v \in T$$

$$f_i^v = \sum_{j=1}^{i-1} \sum_{w \in N(v)} f_j^w * f_{i-j}^v$$

Definition: Let $\mathcal{M}$ be a min sum semi-ring consisting of the set $\mathbb{N} \cup \infty$ and operations min and $+$. We embed M in $\mathbb{Z}[\mathbb{N}]$ with $\oplus$ and $\otimes$. We represent $a \in \mathcal{M}$ by $a' \in \mathbb{Z}[\mathbb{N}]$ such that $a[i] > 0$ for $i = a$ and $a[i] = 0$ for $i < a$. Let b', c' and d' represent b, c and d, respectively. Then

$$\min\{a, b\} = c, a + b = d \iff a' \oplus b' = c', a' \otimes b' = d'$$

Observation: For min sum semi-ring $\mathcal{M}$ the definition of $*_{\mathcal{M}}$ introduces *min sum subset convolution*, $(f *_{\mathcal{M}} g)[X] = \min_{W \subseteq X} f[W] + g[X \setminus W]$.

Theorem 6.1: Let V be a set and w an integer. Let C be a circuit over $(\mathbb{N}[2^V]; \min, *_{\mathcal{M}})$. Let D be obtained from C by replacing all min with max gates and $*_{\mathcal{M}}$ with $\oplus$ gates and all constants with a table containing $w + 1$ in all entries. Suppose all constants of C are singletons and C, D outputs s, t, respectively. Then it can be decided whether $s[V] \le w$ using $\mathcal{O}^*(2^{|V|}u)$ time and polynomial space, where $t[Y] \le u$ for every $Y \subseteq V$.

Problem TRAVELLING SALESMAN PROBLEM
Instance: A graph $G = (V, E)$, vertex s, function $\omega : V \times V \to \{1, \ldots, d\}$ and an integer $t \le |V|d$.
Question: Is there a Hamiltonian cycle $E' \subseteq E$ of weight at most t?

$$f_0^v = [X = \emptyset]\omega(s, v)$$
$$f_i^v = \min_{u \in N(v)} (f_{i-1}^u *_{\mathcal{M}} [X = \{v\}]) + \omega(u, v)$$

Problem WEIGHTED STEINER TREE
Instance: A graph $G = (V, E)$ with weight function $\omega : E \to \{1, \ldots, d\}$, $T \subseteq V$ and an integer $t \le |V|d$.
Question: Does there exist a subtree (V', E') of G such that $\sum_{e \in E'} \omega(e) \le t$ and $T \subseteq V'$?

$$f_1^v = [X = \emptyset] \text{ for } v \notin T$$
$$f_1^v = [X = \{v\}] \min [X = \emptyset] \text{ for } v \in T$$
$$f_i^v = \min_{j=1}^{i-1} \min_{w \in N(v)} f_j^w *_{\mathcal{M}} f_{i-j}^v + \omega(vw)$$